Extra help: Troubleshooting your installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods.

Most methods can be used for both FortiGates in both NAT/Route and Transparent mode. Any exceptions are marked.

1. Use FortiExplorer if you can't connect to the FortiGate over Ethernet.

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.

3. Check the physical network connections.

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device. Also, check the Unit Operation widget, found at **System > Dashboard > Status**, to make sure the connected interfaces are shown in green.

4. Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).

Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.

If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.

5. Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

6. Check the FortiGate interface configurations (NAT/Route mode).

Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure Addressing Mode is set to the correct mode.

7. Verify the security policy configuration.

Go to **Policy & Objects > Policy > IPv4** (or **Policy & Objects > Policy > IPv6**) and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Sessions**, and select **Apply**).

If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is turned on and that **Use Destination Interface Address** is selected.

8. Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).

Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to Internet-facing interface.

9. Verify the static routing configuration (NAT/Route mode).

Go to **Router > Static > Static Routes** (or **System > Network > Routing**) and verify that the default route is correct. View the **Routing Monitor** (found either on the same page or at **Router > Monitor > Routing Monitor**) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.

10. Verify that you can connect to the gateway provided by your ISP.

Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

11. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

12. Verify the DNS configurations of the FortiGate unit and the PCs.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`. If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

13. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, confirm that it can reach FortiGuard.

First, check the License Information widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to **System > Config > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the GUI should show a successful connection.

14. Consider changing the MAC address of your external interface (NAT/Route mode).

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
   edit <interface>
      set macaddr <xx:xx:xx:xx:xx:xx>
   end
end
```

15. Check the FortiGate bridge table (Transparent mode).

When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit. Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed that is a likely cause. Check for the MAC address of the interface or device in question.

To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. Check the device's network connections and make sure they are connected and operational

16. Either reset the FortiGate unit to factory defaults or contact the technical assistance center.

If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

You can also contact the technical assistance center. For contact information, go to support.fortinet.com.